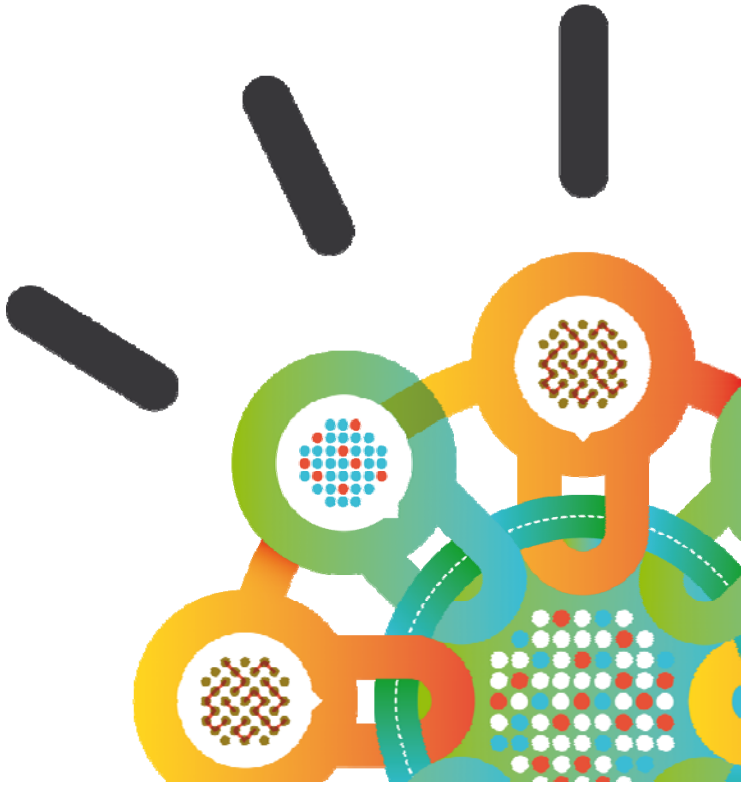
Security Intelligence.
Think Integrated.

IBM Security Network Protection XGS 5000

Introducing IBM's Next Generation of Intrusion Prevention Solutions

Andrew Sallaway
Security SWAT Team
IBM Security Systems



The challenging state of network security

Stealth Bots • Targeted Attacks
Worms • Trojans • Designer Malware

SOPHISTICATED ATTACKS

Increasingly sophisticated attacks are using multiple attack vectors and increasing risk exposure

STREAMING MEDIA

Streaming media sites are consuming large amounts of bandwidth

SOCIAL NETWORKING

Social media sites present productivity, privacy and security risks including new threat vectors

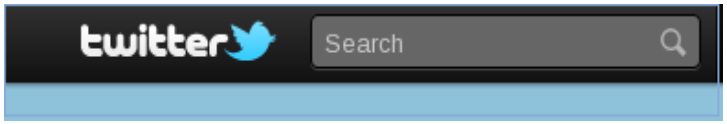
URL Filtering • IDS / IPS
IM / P2P • Web App Protection
Vulnerability Management

POINT SOLUTIONS

Point solutions are siloed with minimal integration or data sharing

Consumerisation of the Enterprise

- Block completely?
  - Some applications are business relevant
  - Not a good look for employers
- Controlled access
  - Shouldn't the marketing department have unobstructed access to facebook and twitter
  - Perhaps we could let employees read their private Email accounts or Facebook between 12noon and 2pm each day?
    - Limit any private email to text only (not files)
    - Only allow “read” of Facebook
- Shouldn't employees be allowed to use Skype for contacting overseas offices?
  - How to handle “thick” client applications



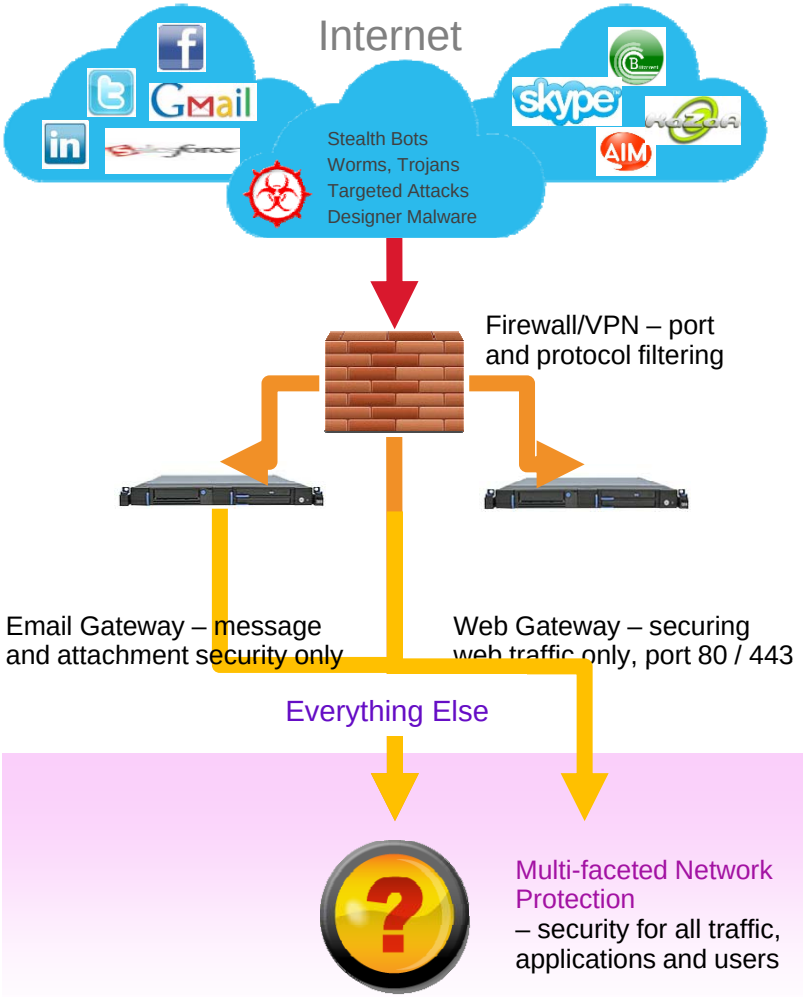
Network Defense: Traditional solutions not up to today's challenges

Current Limitations

- Threats continue to evolve and standard methods of detection are not enough
- Streaming media sites and Web applications introduce new security challenges
- Basic "Block Only" mode limits innovative use of streaming and new Web apps
- Poorly integrated solutions create "security sprawl", lower overall levels of security, and raise cost and complexity

Requirement: Multi-faceted Protection

- 0-day threat protection tightly integrated with other technologies i.e. network anomaly detection
- Ability to reduce costs associated with non-business use of applications
- Controls to restrict access to social media sites by a user's role and business need
- Augment point solutions to reduce overall cost and complexity



The Need to Understand the Who, What, and When

- Server
- Network
- Geography
- Reputation
- User or Group

Web Applications

Non-web Applications

Web Category Protection	Allow marketing and sales teams to access social networking sites
Access Control	Block attachments on all outgoing emails and chats
Protocol Aware Intrusion Protection	A more strict security policy is applied to traffic from countries where I do not do business
Client-Side Protection	Advanced inspection of web application traffic destined to my web servers
Botnet Protection	Block known botnet servers and phishing sites
Network Awareness	
Web Protection	
Reputation	Allow, but don't inspect, traffic to financial and medial sites

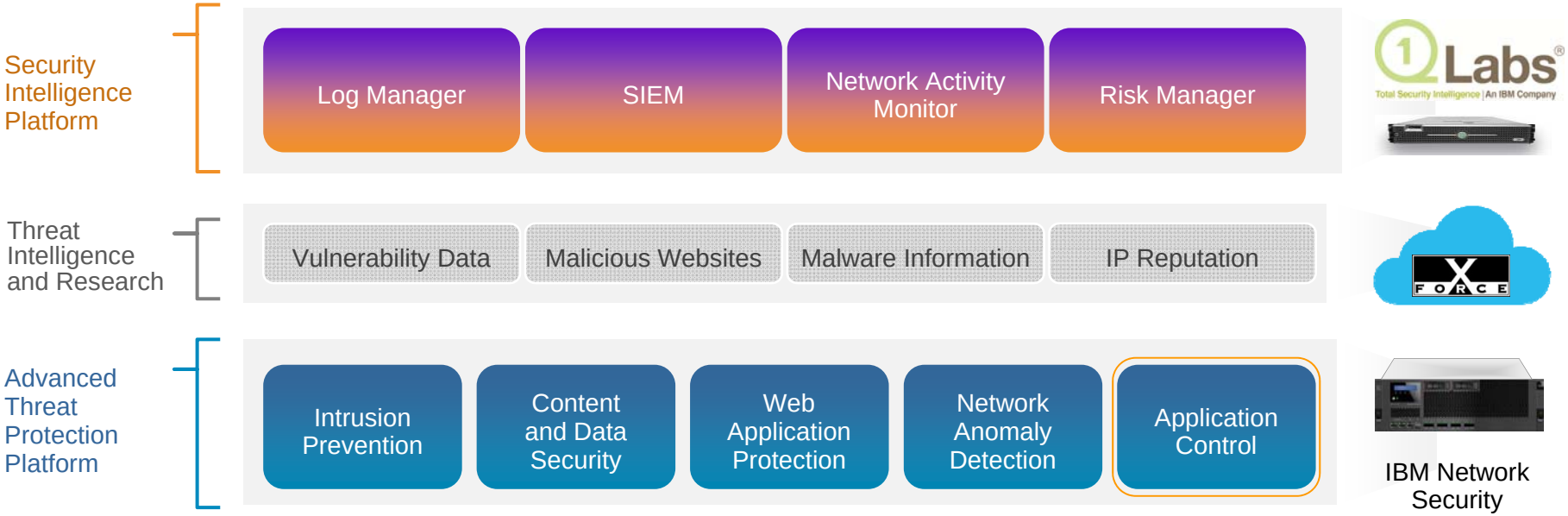
Who → 172.29.230.15, 192.168.0.0 /16

What → 80, 443,25, 21, 2048-65535

Controls → ?

Security

The Advanced Threat Protection Platform



Advanced Threat Protection Platform

Ability to prevent sophisticated threats and detect abnormal network behavior by leveraging an extensible set of network security capabilities - in conjunction with real-time threat information and Security Intelligence

Expanded X-Force Threat Intelligence

Increased coverage of world-wide threat intelligence harvested by X-Force and the consumption of this data to make smarter and more accurate security decisions across the IBM portfolio

Security Intelligence Integration

Tight integration between the Advanced Threat Protection Platform and QRadar Security Intelligence platform to provide unique and meaningful ways to detect, investigate and remediate threats

Introducing **IBM Security Network Protection XGS 5000**

	NEW WITH XGS	NEW WITH XGS
PROVEN SECURITY	ULTIMATE VISIBILITY	COMPLETE CONTROL
Extensible, 0-Day protection powered by X-Force®	Understand the Who, What and When for all network activity	Ensure appropriate application and network use

IBM Security Network Protection XGS 5000
builds on the proven security of IBM intrusion prevention solutions by delivering the addition of next generation *visibility* and *control* to help balance security and business requirements

Proven Security: Extensible, 0-Day Protection Powered by X-Force®

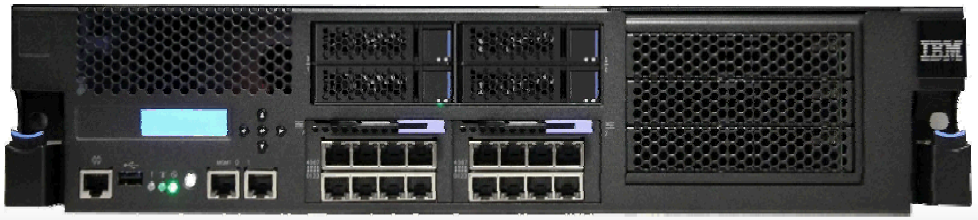
- Next Generation IPS powered by X-Force® Research protects weeks or even months “ahead of the threat”
- Full protocol, content and application aware protection goes beyond signatures
- Expandable protection modules defend against emerging threats such as malicious file attachments and Web application attacks

“When we see these attacks coming in, it will shut them down automatically.”

– Melbourne IT

[The IBM Threat Protection Engine] “defended an attack against a critical government network another protocol aware IPS missed”

– Government Agency



IBM Security Network Protection XGS 5000

IBM Security Threat Protection

- Vulnerability Modeling & Algorithms
- Stateful Packet Inspection
- Port Variability
- Port Assignment
- Port Following
- Protocol Tunneling
- Application Layer Pre-processing
- Shellcode Heuristics
- Context Field Analysis
- RFC Compliance
- Statistical Analysis
- TCP Reassembly & Flow R
- Host Response Analysis
- SIT Tunnel Analysis
- Port Probe Detection

– Backed by X-Force®

– 15 years+ of vulnerability research and development

– Trusted by the world’s largest enterprises and government agencies

– True protocol-aware intrusion prevention, not reliant on signatures

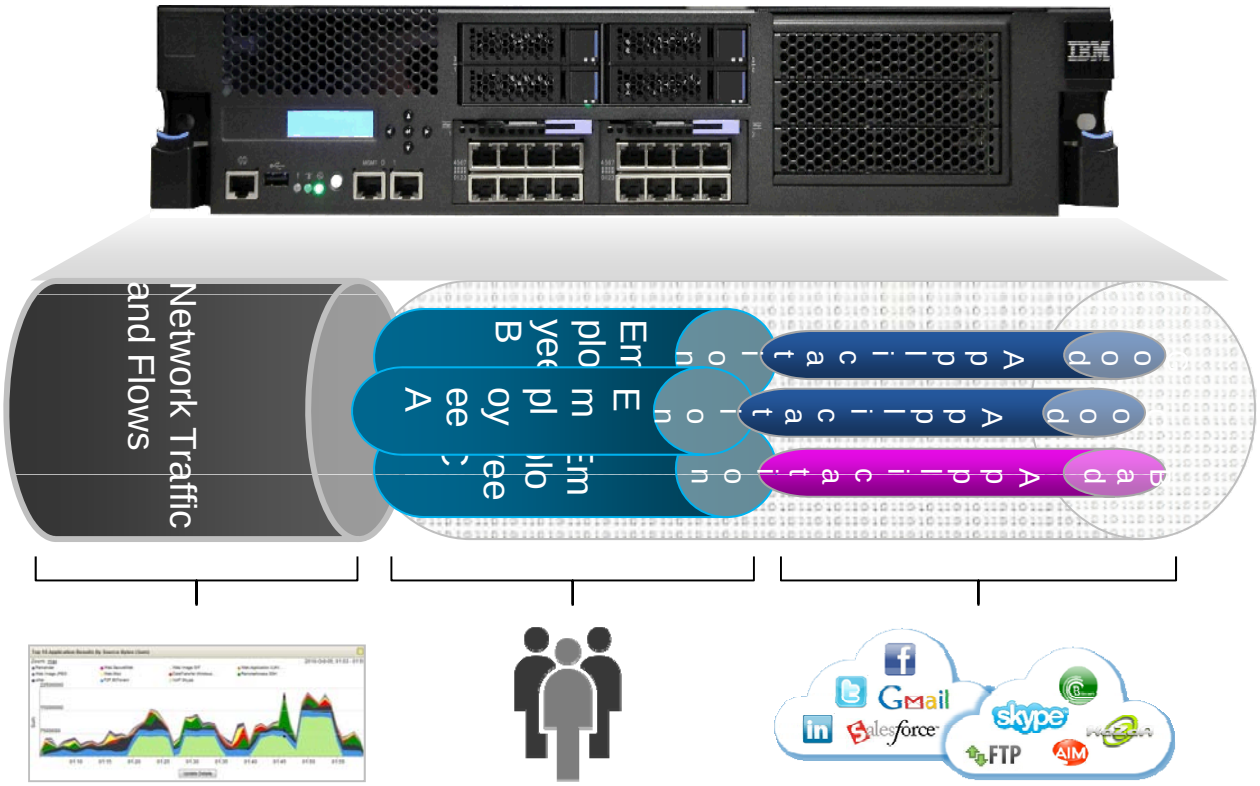
– Specialized engines

- Exploit Payload Detection
- Web Application Protection
- Content and File Inspection

Ability to protect against the threats of today and tomorrow

Ultimate Visibility: Understanding Who, What and When

- Immediately discover which applications and web sites are being accessed
- Quickly Identify misuse by application, website, user, and group
- Understand who and what are consuming bandwidth on the network
- Superior detection of advanced threats through integration with QRadar for network anomaly and event details



Network Flow Data provides real time awareness of anomalous activities and QRadar integration facilitates enhanced analysis and correlation

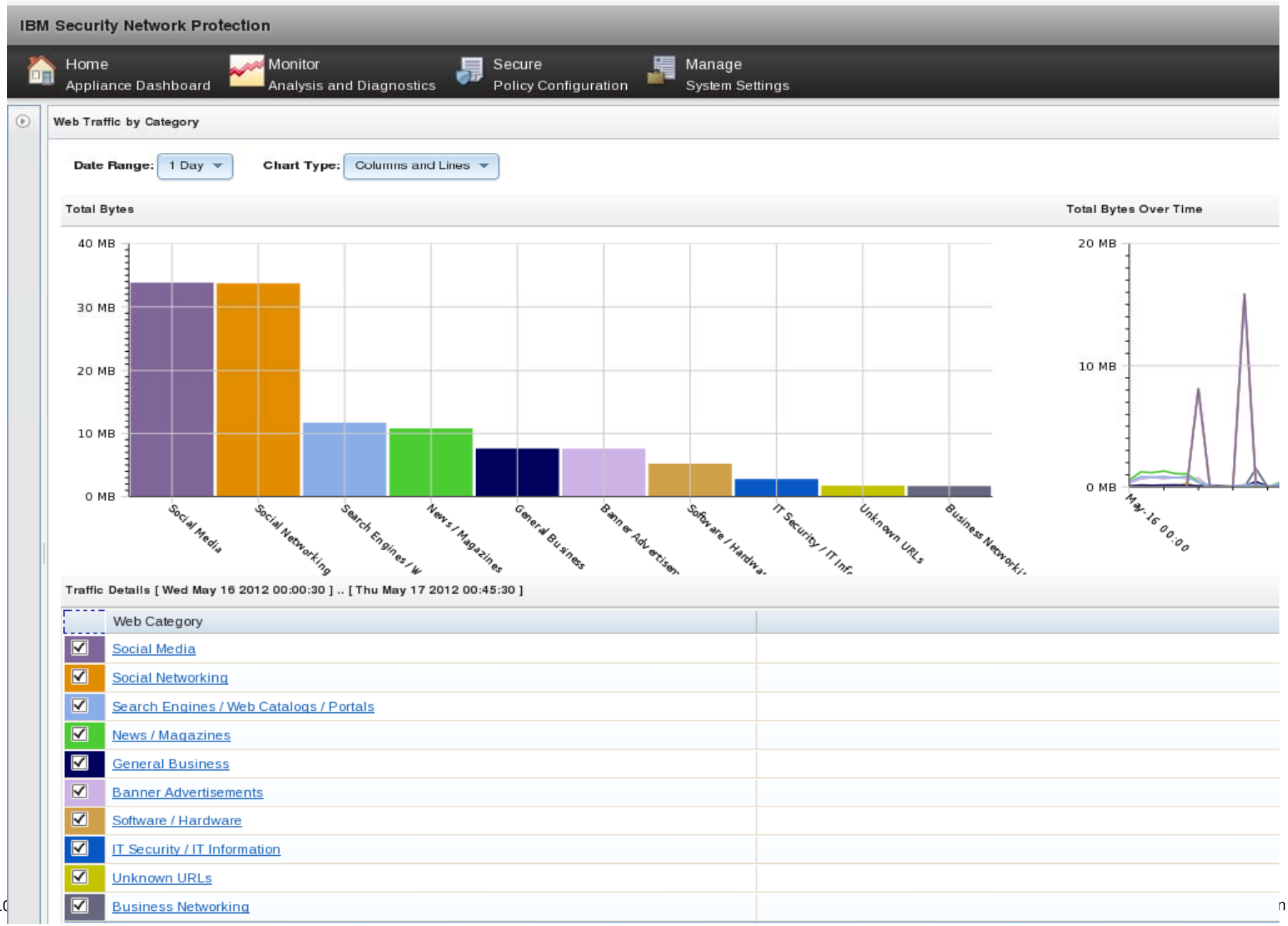
Complete Identity Awareness associates valuable users and groups with their network activity, application usage and application actions

Application Awareness fully classifies network traffic, regardless of address, port , protocol, application, application action or security event

"We were able to detect the Trojan "Poison Ivy" within the first three hours of deploying IBM Security Network Protection"

– Australian Hospital

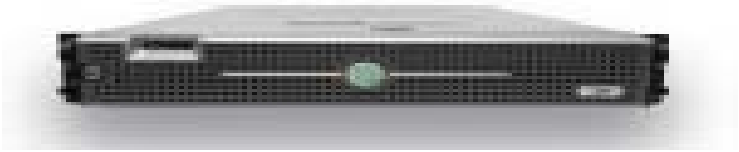
Increase Security • Reduce Costs • Enable Innovation

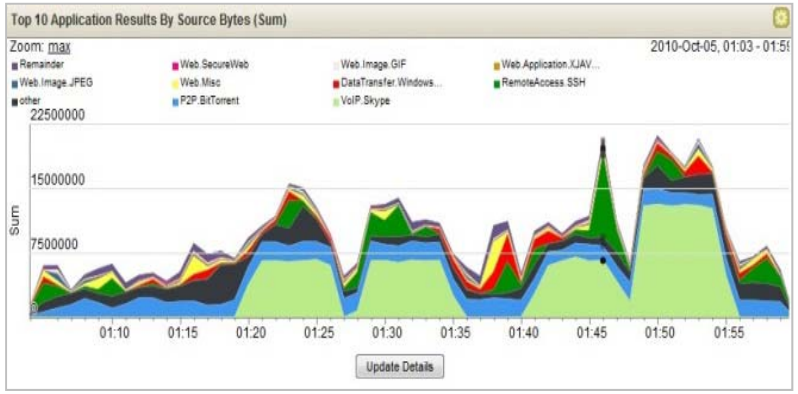

IBM Security Network Protection
Home
Appliance Dashboard
Monitor
Analysis and Diagnostics
Secure
Policy Configuration
Manage
System Settings
Web Traffic by Category
Date Range: 1 Day
Chart Type: Columns and Lines
Total Bytes
Total Bytes Over Time
40 MB
30 MB
20 MB
10 MB
0 MB
Social Media
Social Networking
Search Engines / W
News / Magazines
General Business
Banner Advertisem
Software / Hardwa
IT Security / IT Infr
Unknown URLs
Business Networki
20 MB
10 MB
0 MB
May-16 00:00
Traffic Details [Wed May 16 2012 00:00:30] .. [Thu May 17 2012 00:45:30]
Web Category
Social Media
Social Networking
Search Engines / Web Catalogs / Portals
News / Magazines
General Business
Banner Advertisements
Software / Hardware
IT Security / IT Information
Unknown URLs
Business Networking

QRadar Network Anomaly Detection

- QRadar Network Anomaly Detection is a purpose built version of QRadar for IBM's intrusion prevention portfolio
- The addition of QRadar's behavioral analytics and real-time correlation helps better detect and prioritize stealthy attacks
- Supplements visibility provided by IBM Security Network Protection's Local Management (LMI)
- Integration with IBM Security Network Protection including the ability to send network flow data from XGS to QRadar

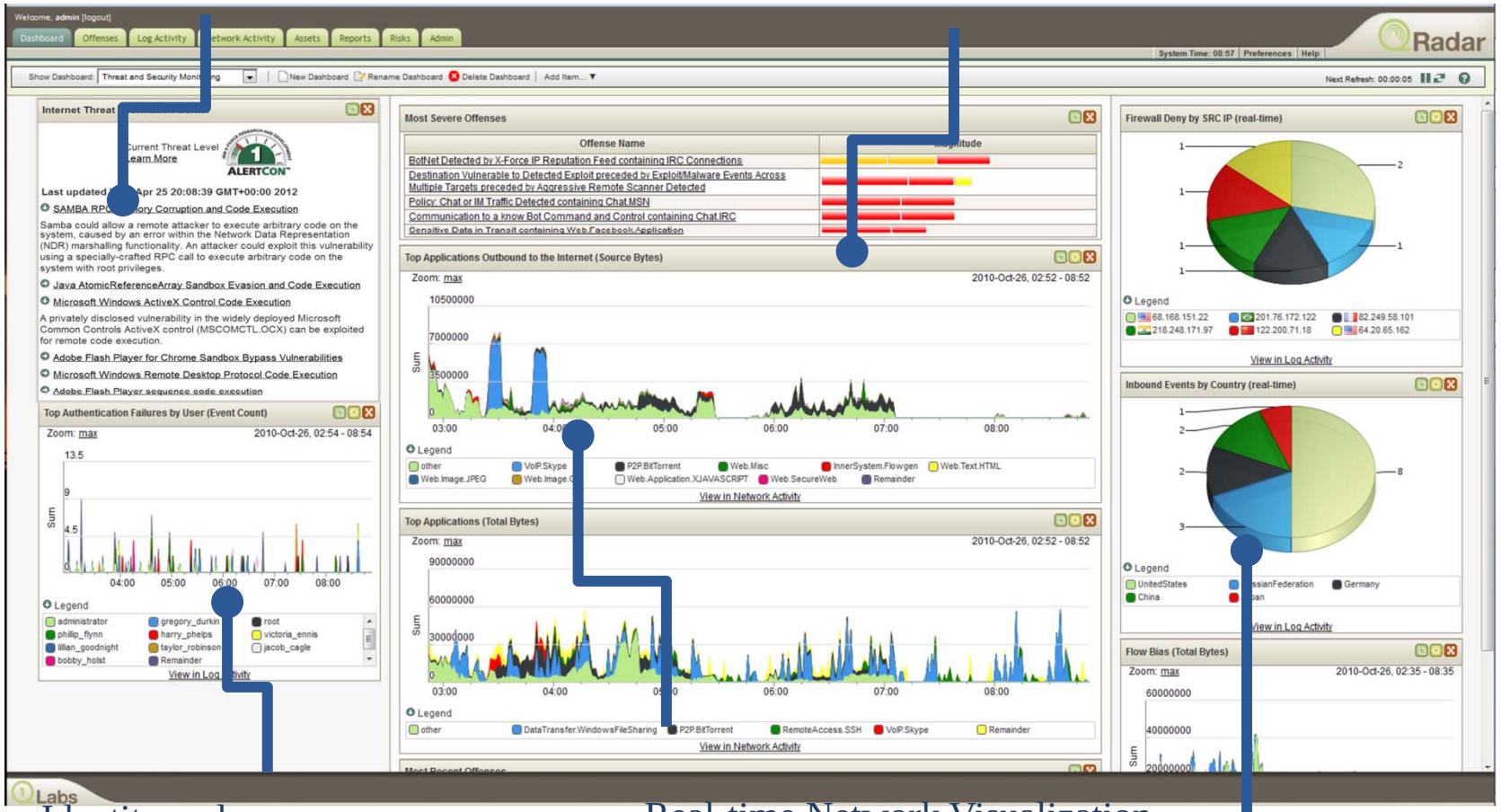
Total Security Intelligence | An IBM Company





IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation



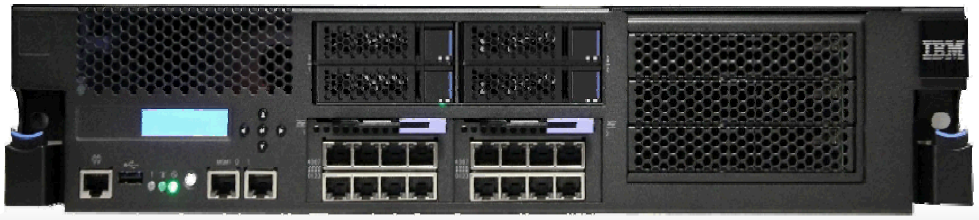
Identity and User Context

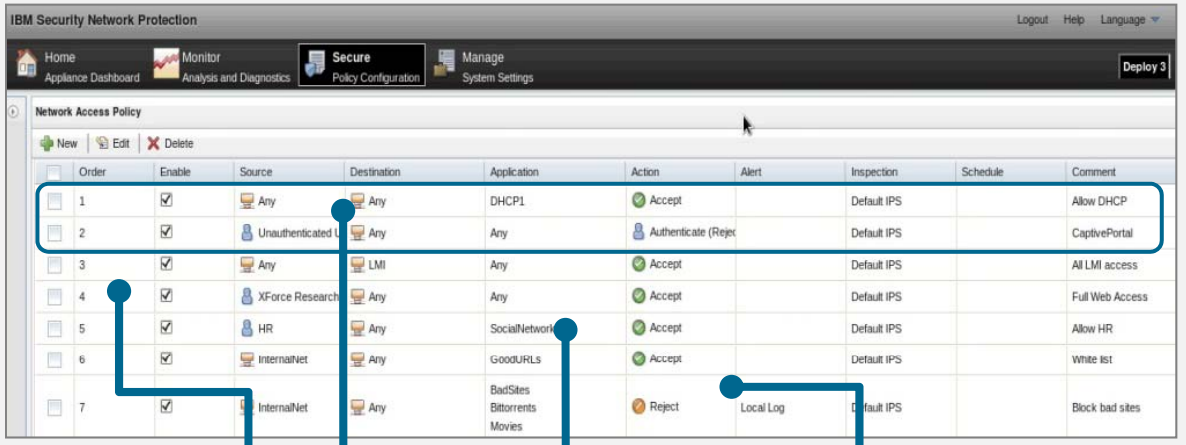
Real-time Network Visualization and Application Statistics

Inbound Security Events

Complete Control: Overcoming a Simple Block-Only Approach

- Network Control by users, groups, systems, protocols, applications & application actions
- Block evolving, high-risk sites such as Phishing and Malware with constantly updated categories
- Comprehensive up-to-date web site coverage with industry-leading 15 Billion+ URLs *(50-100x the coverage comparatively)*
- Rich application support with 1000+ applications and individual actions





Limit the use of social networking, file sharing, and web mail for common users

Allow full access to social networking sites for marketing and HR teams

Stop broad misuse of the corporate network by blocking sites that introduce undue risk and cost

Flexible network access policies controls access to systems and applicable security policy

"We had a case in Europe where workers went on strike for 3 days after Facebook was completely blocked…so granularity is key."

– IBM Business Partner

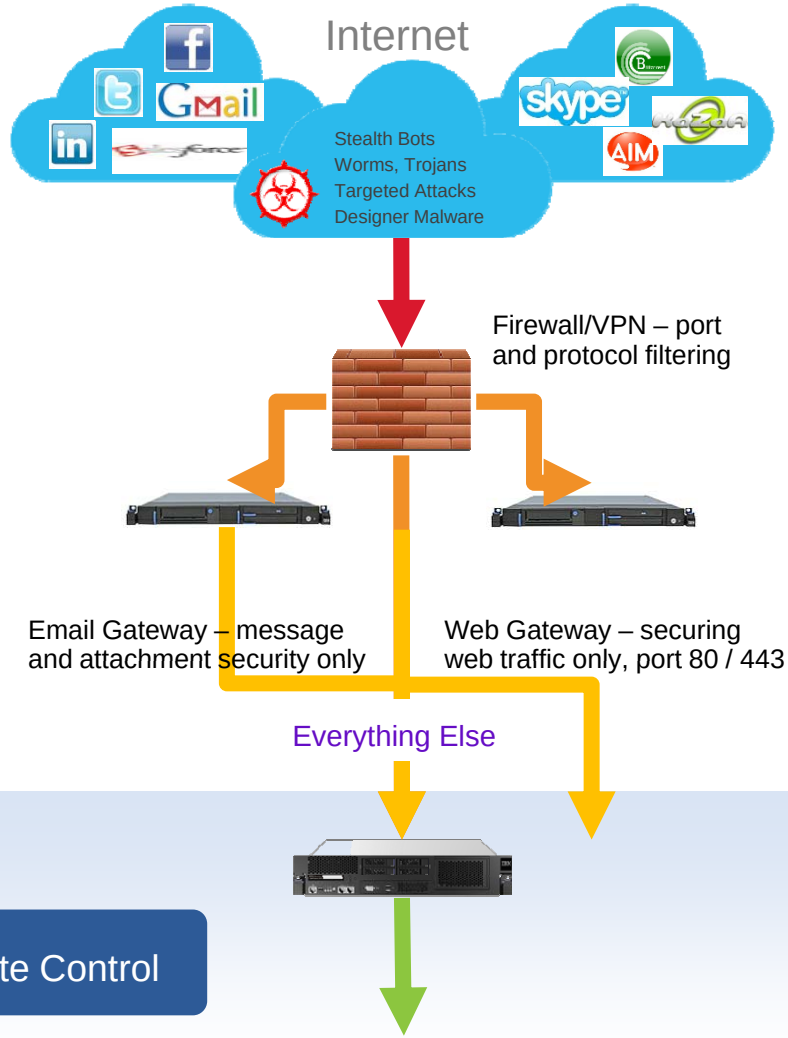
The XGS 5000: The Best Solution for Threat Prevention

Better Network Control

- Natural complement to current Firewall and VPN
- Not rip-and-replace – works with your existing network and security infrastructure
- More flexibility and depth in security and control over users, groups, networks and applications

Better Threat Protection

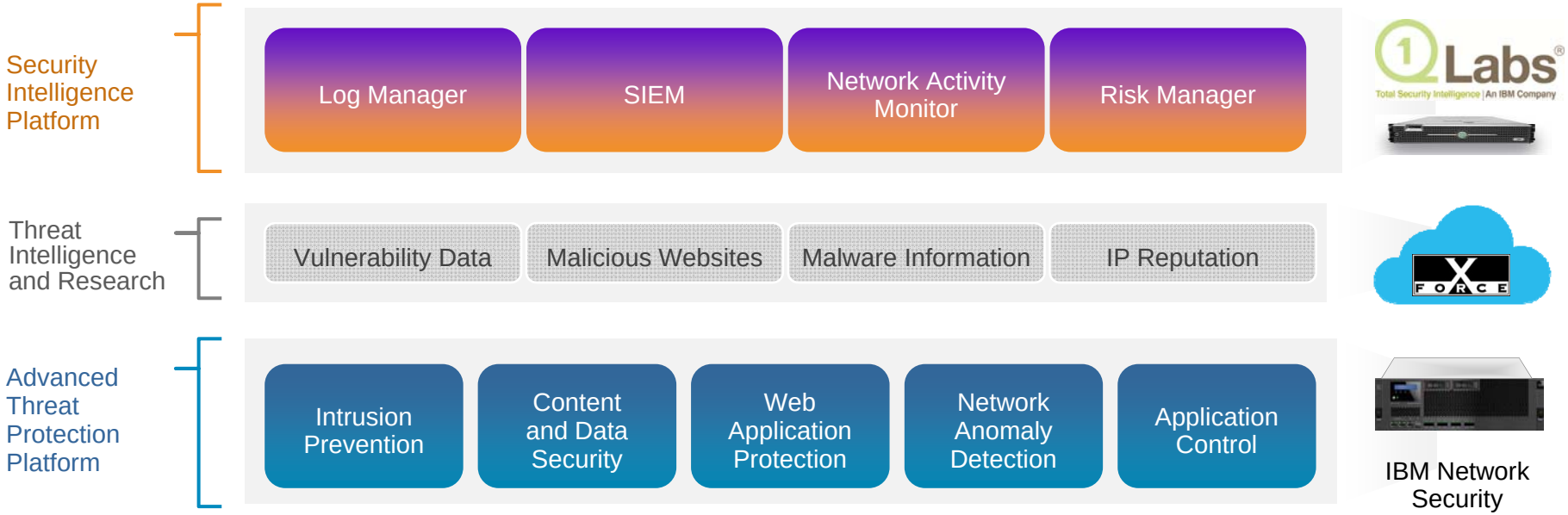
- True Protocol aware Network IPS
- Higher level of overall security and protection
- More effective against 0-day attacks
- Best of both worlds – true protocol and heuristic-based protection with customized signature support



IBM Security Network Protection XGS 5000

Proven Security | Ultimate Visibility | Complete Control

Part of IBM's vision for Advanced Threat Protection



Advanced Threat Protection Platform

Ability to prevent sophisticated threats and detect abnormal network behavior by leveraging an extensible set of network security capabilities - in conjunction with real-time threat information and Security Intelligence

Expanded X-Force Threat Intelligence

Increased coverage of world-wide threat intelligence harvested by X-Force and the consumption of this data to make smarter and more accurate security decisions across the IBM portfolio

Security Intelligence Integration

Tight integration between the Advanced Threat Protection Platform and QRadar Security Intelligence platform to provide unique and meaningful ways to detect, investigate and remediate threats

ibm.com/security